Research Paper | Education | E-ISSN No : 2454-9916 | Volume : 10 | Issue : 3 | March 2024

SECURE CLOUD STORAGE WITH BLOCKCHAIN TECHNOLOGY USING MULTI-KEY AGGREGATION ALGORITHM

Nagamany Abirami[1], Dr. M.S.Anbarasi[2]

[1] Research Scholar, Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India.
[2] Assistant Professor, Department of Information Technology, Pondicherry Technological University, Puducherry, India.

ABSTRACT

Cloud computing is an emerging technology which provides on-demand availability of system resources, especially data storage and computing power. Cloud computing technology helps for reducing maintenance cost, highly available across the globe, flexible and easy scalability. Even though the cloud computing has many useful services, still we have a security challenges on data integrity and privacy. Blockchain Technology is the most important security solutions for the protection of information stored on Cloud.The Internet uses a centralized method of monitoring, critical information in the database has been easily manipulated or disclosed by cyber criminals or cloud organizations.To address this limitation, researchers offer Chain Privacy, a blockchain-based access to information system.First, customers use blockchain network node account information as an identifier and also redefining cloud-based access control permissions, which would be encoded and retained on the blockchain.Subsequently, customer uses Chain Privacy to create network access, authorization, and cancel procedures.With a huge use of cloud services, information security issues still need to be addressed appropriately.Data security issues have always been an obstacle in the development of cloud computing, but they must be addressed.At the same time, Blockchain has established itself as a crucial method to ensure security, in particular in terms of consistency, validity, and confidentiality.This paper proposed the Multi-Key Aggregation Security (MAS) in Blockchain and cloud computing, to improve the performance of security.Finally, Enterprise Operating System (EOS) is used to create Chain Privacy. And the results suggest that Chain Privacy could not only protect cybercriminals and managers against unauthorized access to information, but also preserve approved confidentiality.

KEYWORDS: Cloud Computing, Blockchain, Information Security

1. INTRODUCTION

Cloud users to make customer inquiries to Cloud Service Providers (CSP). CSPs are third-party firms that would provide cloud storage to their clients. Two further third-party suppliers, Third Party Auditor (TPA) and Attribute Authority (AA) was expected to provide security features in the cloud [1]. As we all know, trust and commitment seem to be the most sensitive and important challenges when it comes to cloud benefits for enterprises and organizations. There have been various reasons for all of this, including [2] [3]; cloud customers' information would be at risk of being lost, revealed, or hacked, plus customers would have no way out of the situation. Cloud clients have no idea with whom they were connected or what information they shared. Accessibility would be a major concern as well; cloud clients have no idea who has access to their personal information or whether it has been transferred around within the cloud.Blockchain was a new and growing technology that cloud consumers could apply to increase data security and reliability when freelancing and obtaining services from the cloud. In comparison to centralized data protection, blockchain could provide secure systems. A cryptographic hash method would be used to track how many records have been linked and connected to the previous block [4]. The blockchain was a distributed ledger that could store data while also protecting it from tampering. Because blockchain generally runs on a peer-to-peer network, it was created to be resistant to manipulation. Information security in the blockchain may be comparable to a centralized database. Information gathered problems, and threats, could be avoided from a strategic point of view. Moreover, the Blockchain does have a good quality, this could give information sharing when used to a place that required information declaration.It might be used in a different domain, along with a finance industry and the Internet of Things (IoT) ecosystem, and its implementations were likely to grow as a result of its advantages [5-9]. Because of its speed and accessibility, cloud- computing was indeed embraced by several IT systems. moreover, a major safetycomponent of cloud confidentiality plus protection was indeedaddressed [10].

2. RELATED WORKS

Furthermore, for identifying, passwords, authorization, log-in details, and so on, they both seem to have a centralized collection and administration methods. As a result, the access control technology has still two privacy and security issues [11-13]:

1. 1) An outside hacker hits the trustworthy center, tampering with the approved information on the centralized computer and illegally accessing or stealing the assets cloud storage by customers.
2. 2) Because the cloud network manager has been in charge of the permission information and seems to have the authorization to view and administer the services, a hostile cloud network manager would use this authority to get unauthorized access to the information by interfering with

the permission information.

To address the aforementioned issues, researchers offer Chain Privacy, a blockchain-based authorization architecture with cloud privacy protection [14-16]. The following were our suggestions:

- Framework for decentralized network access. Chain Privacy Stores access management controls the decentralized and tamper-proof blockchainand utilizes the blockchain profile number as the identification before designing the network access, permission, and permission cancellation procedure.
- Approved handling of personal data. It was simple to reveal consumers' privacy thanks to blockchain's openness. Customers' private was efficiently protected by Chain Privacy, which encodes and saves accessing management control in the blockchain.
- Safety and protection. Chain Privacy not only ensures the assets' privacy, authenticity, accessibility, validity, and responsibility but also protects them from cyber threats.

3. BLOCKCHAIN TECHNOLOGY

A block's architecture is depicted in Figure 1.A component in Blockchain often comprises the important data, such as the hashes of the previous and present blocks, the date, and other information.

The most important information would be: depending on the different types of services given by a block-like as bank undertaking records, connection records,space documents, or IoTinformation files, the price varies.

Hash: next the transaction takes place, which must be hash and given out to certain other servers. Because each node cell holds thousands of transactional data and the last hash to block headers, blockchainworkers the Merkle tree method to reducenetwork infrastructure and computation requirements.

Timestamp: The distance of period it took to create a block.

Additional data: Other data include block stamps, user-specified information, and once rates, among many other things

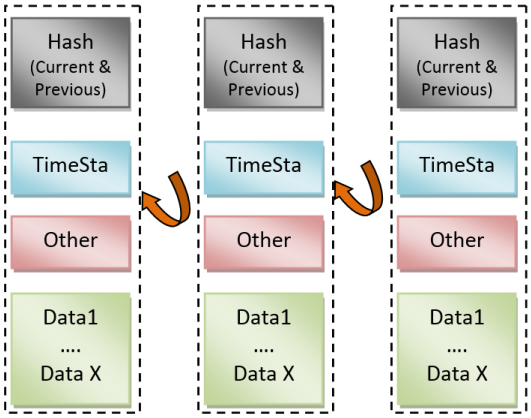


Figure 1: Blockchain structure

A blockchain block contains a block effect on the body by a preceding block, as shown in Table 1. Block version, Parents block password, Merkle tree root hash, Timestamp, n Bits,and the Nonce value was included in the block header. The block consists of the prologue it contains block data, an earlier block secret hashes together with the secret hash, and a listing of transaction information. The "Block Height" depends on the number of operations present in each block, which was 500. The normal size of each exchange was 250 bytes, although the block header was 80 bytes.

Type	Size	Description
Block Header	82	Block header data
Counter	1-10	Number of transactions
Block Size	5	Size of the block

Table 1: Block information of blockchain

A. Requirement of Cloud

Among the most critical Cloud Needs that could affect different Cloud design approaches.

- Scalability: The Cloud Network was capable of handling millions of customers or nodes who use Cloud services. In terms of volume, the developed system was flexible, with units that might be expanded from one to another.
- Elasticity: The intelligent blockchain technology could alter the work by pre-programming asset allocation and allocation, ensuring that all capabilities continue to meet current needs to the best of their abilities.
- Confidentiality: All customers must have efficient control over the information, which should be protected by the network.
- Infinite Computing Resources: Clouds' provisioning services do not require customers to formulate a strategy.
- Pricing: Various Cloud services and applications have various prices, and pay, was based on capacity use.
- Utilization: Abilities could be changed effectively for good changing pressure by allowing the most effective use.
- Cost-effectiveness: The cloud services were network-based, making them convenient for individual customers, as they would not require users to purchase the software that had been applied to the equipment. As a result, the total cost of program conservation and management would be lowered.
- Evaluations are often measured in terms of the efficiency of the apps and services operating on the cloud system.
- Flexibility: This refers to the capacity to share files or resources across the web. Customers benefit from additional freedom thanks to the cloud.

B. Challenges for Blockchain Security

Blockchain technology, as we all understand, was closely tied to computer-generated and a digital currency and has been used by everyone. However, various Blockchain safety problems have been reported, including the following:

a) Blockchain Agreement: A Blockchain would be a set of consecutive connections of fundamentally formed blocks. A Blockchain could be separated because the last two blocks

created momentarily could be used by two separate customers if 2 distinct competitors achieved a conclusion at the same period while extraction. If the newest block isn't chosen by the members in the Bitcoin network, the block becomes irrelevant, and ongoing mining becomes meaningless. The system would monitor Bitcoin competitors with a processing capability of greater than 50 percent.

b) Transaction Security: To solve safety problems, several transactions forms could be constructed utilizing a dynamic computer language and a very well screenplay for outputs and inputs. The Bitcoin agreement would be used for financial institutions, confirmation, including affirmation. A most typical way of creating an agreement would be to utilize a program that incorporates a multi-user numerous methodology.

*c) Wallet Security:*The hash function of a master password is used to encode the Bitcoin address, which would be encoded with a combination of personal and user friendly. As a result, without an unlocking program that determines the value obtained by combining a unique code and a personalized key, the Bitcoin transaction locking program location cannot be unlocked. Inside the Bitcoin wallet was data collected like the address and name private key, which would be utilized to generate the unlocking script. That would be to say, if people lost data within the account, clients would lose Bitcoin since we all understand how important data would be when using Bitcoin. As a result, the Bitcoin wallet becomes the primary target of a Bitcoin hacker assault.

d) Software Security:The technology utilized in Bitcoin seems to be a key cause of worry, as a defect in the program could be disastrous. Although the Bitcoin programmer instructions appear to describe all associated Bitcoin operations, the core program of Bitcoin seems to be very skilled and powerful, as the specific procedures of the original Bitcoin software were guided and produced utilizing Satoshi Nakamoto's technology.

4. PROBLEM STATEMENT

When academics were studying the 3 types of cloud access control systems or cloud network access, there are two consistent features:

a) One or more trusted centers: Cloud technology access controls, encrypted communication authorization designs, including virtualization user access designs, as presented by the professor, all need one or more authorized countries to maintain names, passwords, authorization powers, and so on. The UCON-based solution, for example, needs trustworthy centers to maintain access privileges, including admin privileges, responsibilities and circumstances in the internet access control mechanism. Secondly, unlike cryptographically network access, ABE-based access management necessitates the administration and distribution of keys by one or more authorized centers. Lastly, in virtualization, network access, store virtual machine (VM) authorization privileges in a trusted center. Furthermore, industry-standard cloud access control necessitates the use of a recognized center to hold client identification information including access rights.

b) Internal trusted system administrator (SA): Customers could choose from three types of cloud services: IaaS, PaaS, and SaaS. Even though companies offer various services, they all require an internal trusted SA to control access control policies. IaaS, for instance, primarily delivers computer processing and memory capacity to consumers while also requiring SA to control and maintain accessibility to conditions. PaaS primarily offers users a platform for designing and delivering application forms, and SA has been responsible for monitoring and managing the product's network access; SaaS primarily provides its users with the application areas people necessitate, and SA has been responsible for managing and maintaining the product's access permissions.

5. SECURE CLOUD WITH BLOCKCHAIN

If consumers' private information gets exposed to the cloud computing environment, this could result in financial and emotional damages. In the cloud services context, researchers primarily investigate information security while sending and storing, like authenticity and confidentiality. If blockchain was improved to a suitable level of service and integrated with the cloud computing system, it could provide safety. A secured e-wallet was created when Blockchain technology has been used. If the e-wallet is not securely erased, the user data may be abused. The participant's leftover information can be analyzed to retrieve the customer's data. Duplicate Blockchain transactions and block the record of Bitcoin poses anoutstanding problem.

To distribute with the safety problems, they have required stable and safe e-wallets.Normally, e-wallets placed on PCs were used, but themobile, phones become more general, which would be very important than an ever carefulassessment of safety from e-wallets in handheld implement. As an outcome, a transaction would be completed when the precision, and the integrity of the data stamp generated to a smartphone, assures the total undertaking safety.a comprehensive perspective of cloud network access could abstract four entities, as seen in Fig. 2: CSP, data user (DU), data owner (DO), and SA, which manages the Access Control Policy Database (ACPD).

When it comes to cloud network access, there have been two issues that arise as a result of the two qualities listed above:Outside Aggressors Interfere with ACPD: Issue 1: Outside Aggressors Interfere with ACPD: Hackers compromise trustworthy authorization centersand interfere with the ACPD system, triggering information spillage or information theft. For example, a hacker may steal ACPD and imitate an authenticated person to gain access to or steal resources, or a hacker may tinker with ACPD by increasing authorizations for unauthorized access or deleting legitimate access permission, compromising privacy and security,

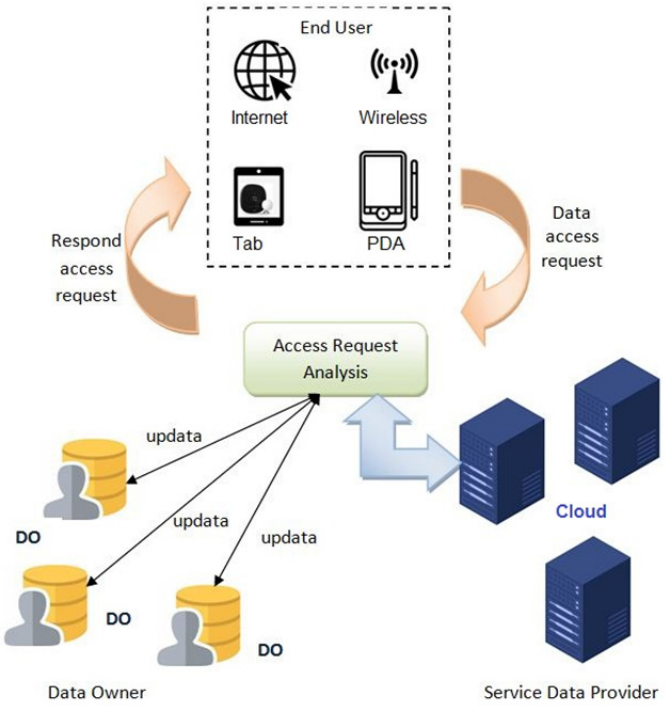


Figure 2: Cloud access control framework

A secured e-wallet should be built by minimizing, validating, including confirming issues that may arise throughout the design, requirement gathering, development, including certification stages, and during management. If the safety of the e-wallet was breached or infiltrated by the assailants, a robust security recovery for an e-wallet must be incorporated. This should maintain the security of capacity to conduct data collected in the e-wallet, & the parameters needed to handle and stimulate an e-wallet. Whenever the e-wallet was that isn't being used, it should have provided a way to efficiently and securely retrieve the remaining customer data, and then delete the rest of the data. Figure 3 depicts the model of the system.

Algorithm: Multi key aggregation security
Step 1: Define key agreement and distribution.

Step 2: (1st level of security) Admin of block chain request for trapdoor keyTn to the user. If the user provides the trapdoor key, then verify the trapdoor key with organization.

Step 3: In the case of a new user, register the web portal and retrieve the trapdoor key.

Step 4: (2nd level of security) Every transaction the block chain admin provides the unique key Un to the user after validation of the trapdoor key.

Step 5: At each transaction the user can get new unique key to access the file on the cloud.

Step 6: The file which is uploaded/updated in the cloud is aggregated with the respective unique key provided by the blockchain.

$File_n = T_n + U_n$ Where n ranges from 1 to n

Step 7: The organization can track the file updation through multikey aggregation

Step 8: If the file found in the cloud then decrypt the key which is attached with the file and block it.

Step 9: (3rd level of security) Then block is added with the blockchain to create the hash id for the updated file.

Step 10: Hash id is generated the URL for the respective file and updated in the block chain admin.

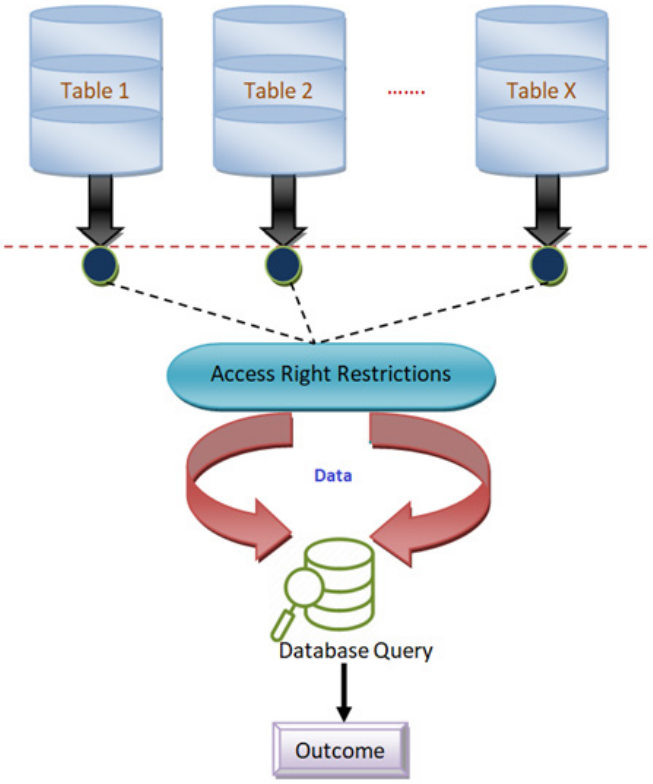


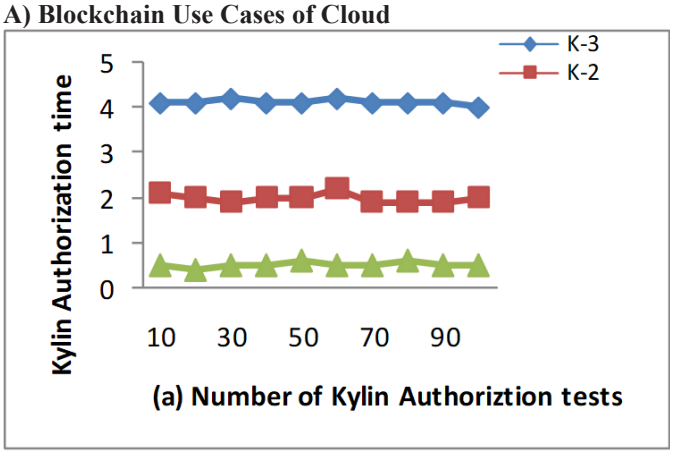
Figure 3: Access Control model

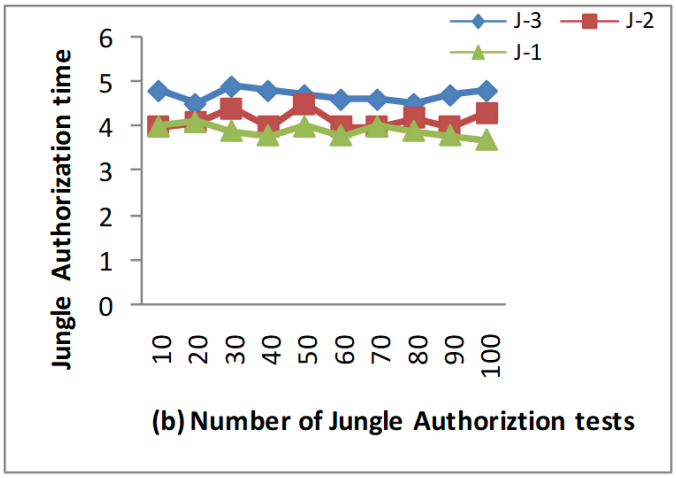
6. PERFORMANCE EVALUATION

Concentrate on-time delivery cost in the AuthPrivacy assessment. Identification verification, permitting, entry authority, including audits have all been aspects of the overall entry management system. Ability to connect must query ResCap S in blockchain with multi key aggregation and validate permission in Chain Privacy provides an authentication system. Clients first examine the hash cost burden, because the hash function result was employed as a unique number, which might also impair query efficiency.Secondly, the permission burden must be examined. Clients put it to the test on mainly two EOS public testing networks, Rainforest and Kylie, with 3 main types of nodes being evaluated on every test chain. Figure 4(a) shows the authorization cost in three network nodes for Kylie; the node of K-1 (api-kylin.eoslaomao.com) for Kylie does have the greatest average efficiency. Figure 4(b) shows the authorization cost in three network nodes for Rainforest; node J-2 has the greatest average efficiency. The

results of the experiments demonstrate that the performance of the authorization publication was dependent on the blockchain chosen and the nodes connecting the blockchains.The speed would be substantially improved by choosing the optimum blockchain and setting the networks. Figure 4(c) shows that Forest's optimum efficiency would be around 4.4s, Kylie's optimum efficiency would be around 0.4s, and the local host's optimum efficiency would be less than 0.02s. These nodes may have multi key aggregation information packets collected by some networks their connections. The node does not create a single information packet receiving from several packets, because the information messages have been aggregated by multi key aggregation. So, for example, n can take the overall median on all incoming numbers their entire environment, but also combine them into a single packet. Each node shall communicate as often as possible in accordance with this original requirement. This next requirement specifies because any drain aggregates any data type information package.

A) Blockchain Use Cases of Cloud





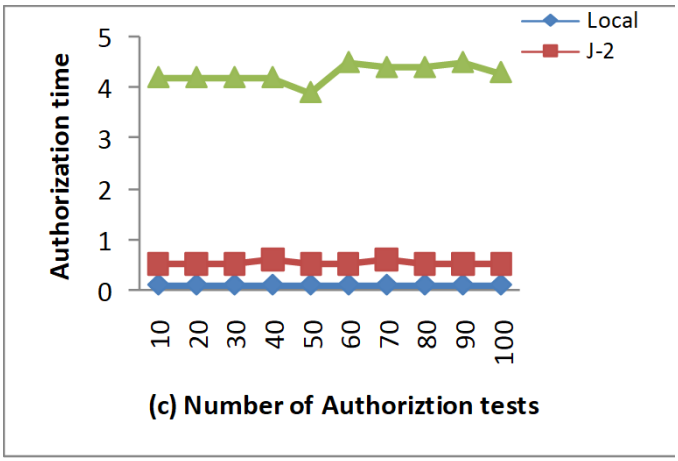


Figure 4: Result analysis

B) Open Ledger: The Cloud technology used by Blockchain was public and available to all users, who can observe all of the cloud's capabilities, including service level agreements (SLAs). The security level that Cloud would supply and offers were visible to all users. Cloud consumers can choose to select their desired required services without needing any additional payment because of the amount of openness and public requirements.

C) Distributed Ledger: Every financial version seems to be in sync, and all cloud customers have access to save the edition of the book. The blockchain keeps track of the resources used by particular cloud customers and quality of service utilization. According to the creator of Policies and SLAs, cloud users standardize their books and records by employing the theory of Bitcoin miners.

D) Decentralized: Standard Defining would be a word used in Blockchain to describe software that keeps track of the terms of this agreement, verifies them, and executes them. CSP, TPA, and AA parties, could have more confidence and openness thanks to the blockchain and smart agreement technology. Implementations were kept on the Blockchain, which would be accessible to all cloud users. The service was contracted once the payment has been confirmed. All contractual activities, and the whole audit trail of events, were saved in chronological order on the Blockchain for future reference. Any entity attempting to alter an agreement on the Blockchain will be detected and prevented by all other cloud users. The average access performance was depicted in Figure 5 (a). When executing reading operations, does have a slight lag. Permission to write performance was depicted in Figure 5(b).

Figure 5: Performace measures

7. CONCLUSION

The study findings of someone using blockchain to tackle the personal private network access in the cloud have been few among safety challenges of the existing blockchain plus cloud. Since most cloud data access controls have one or more authorized centers and trusted inside managers, they were extremely vulnerable to both internal and external threats. This

study proposes an authorization framework Chain Privacy with data protection in the virtual environment to tackle the issues of hackers gaining unauthorized access to cloud resources. The customer posts all authorization-related transactions on the network.The general architecture of Blockchain has indeed been considered in this section. The properties of Blockchain, and Cloud Computing security requirements, were also investigated. Actualizes the framework system based on the EOS blockchain, which considers appropriate access and other metadata to be a separate representation of blockchain transactions. Only users with access privileges could access information, according to the outcomes of the trial. As a result, our system could provide secrecy, consistency, reliability, validity, and responsibility, and prevent assaults from both internally and externally.Based on this analysis, it has been established that Blockchain can be a suitable and powerful tool to provide security in the Cloud Computing environment. Further, this paper reviewed the various existing blockchain implementations for cloud security.

REFERENCES

1. Inukollu, V. N., Arsi, S., &Ravuri, S. R. (2014). Security issues associated with big data in cloud computing. International Journal of Network Security & Its Applications, 6(3), 45.
2. Cardenas, A. A., Manadhata, P. K., &Rajan, S. P. (2013). Big data analytics for security. IEEE Security & Privacy, 11(6), 74-76.
3. Vanga, M. S. R., Vijayaraj, J., Kolluru, P., &Latchoumi, T. P. (2022). Semantics-Driven Safety Measures in Distributed Big Data Systems on IoT. In Advanced Computational Paradigms and Hybrid Intelligent Computing (pp. 251-259). Springer, Singapore.
4. Terzi, D. S., Terzi, R., &Sagiroglu, S. (2015, December). A survey on security and privacy issues in big data. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 202-207). IEEE.
5. Mohammad, A. S., & Pradhan, M. R. (2021). Machine learning with big data analytics for cloud security. Computers & Electrical Engineering, 96, 107527.
6. Tan, Z., Nagar, U. T., He, X., Nanda, P., Liu, R. P., Wang, S., & Hu, J. (2014). Enhancing big data security with collaborative intrusion detection. IEEE cloud computing, 1(3), 27-33.
7. Moreno, J., Serrano, M. A., &Fernández-Medina, E. (2016). Main issues in big data security. Future Internet, 8(3), 44.
8. Lo'ai, A. T., &Saldamli, G. (2021). Reconsidering big data security and privacy in cloud and mobile cloud systems. Journal of King Saud University-Computer and Information Sciences, 33(7), 810-819.
9. Matturdi, B., Zhou, X., Li, S., & Lin, F. (2014). Big Data security and privacy: A review. China Communications, 11(14), 135-145.
10. Thota, C., Manogaran, G., Lopez, D., &Vijayakumar, V. (2017). Big data security framework for distributed cloud data centers. In Cybersecurity breaches and issues surrounding online threat protection (pp. 288-310). IGI global.
11. Bahrami, M., &Singhal, M. (2015). The role of cloud computing architecture in big data. In Information granularity, big data, and computational intelligence (pp. 275-295). Springer, Cham.
12. Sekaran, K., Rajakumar, R., Dinesh, K., Rajkumar, Y., Latchoumi, T. P., Kadry, S., & Lim, S. (2020). An energy-efficient cluster head selection in wireless sensor network using grey wolf optimization algorithm. TELKOMNIKA, 18(6), 2822-2833.
13. Dave, D., Meruliya, N., Gajjar, T. D., Ghoda, G. T., Parekh, D. H., &Sridaran, R. (2018). Cloud security issues and challenges. In Big Data Analytics (pp. 499-514). Springer, Singapore.
14. Majhi, S. K., &Shial, G. (2015). Challenges in big data cloud Computing and Future Research Prospects: a Review. SmartCR, 5(4), 340-345.
15. Latchoumi, T. P., Ezhilarasi, T. P., &Balamurugan, K. (2019). Bio-inspired weighed quantum particle swarm optimization and smooth support vector machine ensembles for identification of abnormalities in medical data. SN Applied Sciences, 1(10), 1-10.
16. Garikapati, P., Balamurugan, K., Latchoumi, T. P., &Malkapuram, R. (2021). A Cluster-Profile Comparative Study on Machining AlSi 7/63% of SiC Hybrid Composite Using Agglomerative Hierarchical Clustering and K-Means. Silicon, 13, 961-972.